REMARKS

Claims 1, 3 and 6-38 are now present in the application.

The Examiner has rejected claims 1, 3, 7, 11, 13-14, 18, 22-23, 29-34 and 36 as being unpatentable over Leo, (a published application, published in 2004) in view of Smith (35 U.S.C. 103 (a)). Applicant respectfully requests reconsideration of this rejection. The Examiner details at pages 3-4 of the Office Action, with respect to claim 1, his support for his position noting that "Leo does not explicitly disclose wherein said verifying mode signs a certificate related to said new entity" and relies on Smith as disclosing "verifying node signs a certificate related to said new entity" (Smith, col. 10, lines 37-53) and concluding based on his interpretation of the references that it would have been obvious to have included in Leo the aforesaid feature of Smith because by verifying the correct signing and formation of these certificates and by verifying that these certificates attest to the public key the device allegedly owned (Smith, col. 4, line 5-8)."

Leo does not teach nor suggest the invention as herein claimed. Leo provides a method and apparatus for managing a sharing of data between a plurality of client units and a corporate server located on a network involving authenticating a client unit with a central management server.

> the authenticating comprising the providing of an identification of the client unit to the central management server, providing from the client unit to the central management server an identification of a corporate server to which the client unit wishes to communicate, providing from the central management server to the client unit an address on the network of the location of a suitable secure bridging unit using at least one of the identification of the client unit, providing a message to communicate to the suitable secure bridging unit from the client unit, said message comprising said identification of the corporate

> server to which said client unit wishes to communicate and data to provide to said corporate server and if said message to communicate with the suitable secure bridging unit is accepted by said secure bridging unit, transferring at least one part of said message to said corporate server, whereby the use of the corporate server and the secure bridging unit enables a control of the communication between the client unit and the corporate server.

(¶0011; *see also* ¶¶ 0012 and 0013 and Fig. 1).

There is no teaching of a distributed authenticated infrastructure such as in the invention and in particular no teaching of where said centralized authentication infrastructure is later integrated into said distributed authenticated infrastructure.

At ¶ 0051 of Leo, the central management server is described in detail and it can be appreciated that the described central management server is not included in a centralized authentication infrastructure integrated into a distributed authentication infrastructure the same including a central server as described by applicant. As set forth in the specification and claims the distributed authentication infrastructure is initially implemented and the centralized authentication infrastructure is later integrated into the distributed authenticated infrastructure after the distributed authentication infrastructure has been established. Fig. 1 of the drawings clearly shows the relationship of the distributed infrastructure the centralized infrastructure and of the central server in the system.

FIG. 1

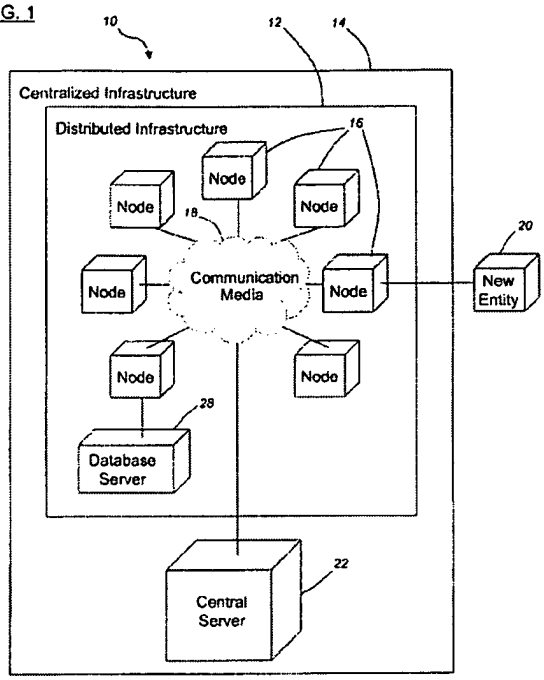
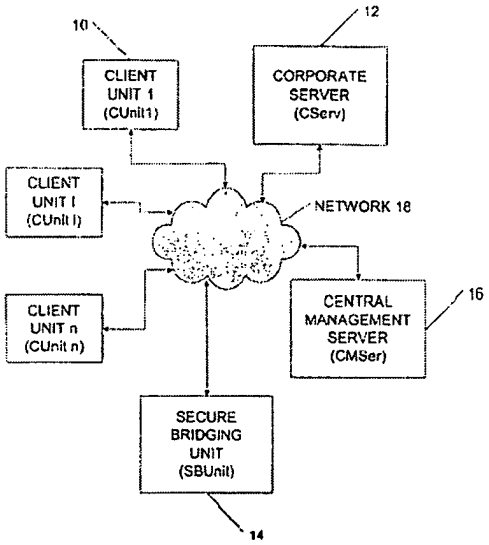


Fig. 1 of Leo, which follows, makes clear the difference in systems:



Aside from the very different systems involved, the system of Smith relied by the examiner as disclosing, "verifying node signs a certificate related to said new entity is entirely different in structure and principle of operation. According to Smith, the certifying authority is a central authority that is trusted by all parties that need to trust the provable untampered stable assuredness of a secure device."

> Identifying and having this authority be the manufacturer of the device offers several natural advantages. Firstly, since the manufacturer bears responsibility for the untampered state of the circuitry and permanent firmware in the device, all parties need to trust the manufacturer anyway. Secondly, the certifying authority must be one that possesses both the motivation and the ability to determine whether a device (without provable untampered state assuredness) is indeed genuine and untampered. The manufacturer, having just built the device, is in the best position to assert this.
>
> Once the `certifying authority` has been identified the device goes through the steps of `initialization`, `keypair generation`, `certification`, `shipment and use`. Some devices also go through the steps of `regeneration` and/or `recertification`. Initialization is performed in the presence of the certifying authority, whereupon the device has its tamper-response circuitry enabled. From this point onward, the device zeroizes its secrets upon tamper.
>
> Generally, keypair generation follows initialization, whereupon the device generates, or requests, a truly random key pair. This may employ RSA, DSS or any other public-key or authentication algorithms. The keypair includes a private key and a public key. The device retains the so generated private key within secure memory. Often, the keypair is generated using an internal source of real, nondeterministic randomness. This is followed by certification, wherein the device then exports its public key to the certifying authority, in a way such that the authority can verify that the public key did indeed emerge from the alleged device. A simple way to do this is in a clean room at the manufacturing facility.
>
> The certifying authority assembles a certificate containing the device's public key, and any desired relevant identifying

> information about the device and its properties. The authority signs this certificate with its own private key, then returns it to the device. The device is ready for shipment and use. From this point onward, the device has the ability to prove that it is untampered by demonstrating that it knows the private key matching the public key contained in the certificate.

Smith, Col. 5, lines 16-55.

The use of an outside certifying authority as expressly required by Smith (see col. 6, lines 45-51; col. 10, lines 37-53; and col. 5, lines 51-55) is alien to both the Leo system and the applicant's system and the cited procedure would not and could not be integrated into Leo. Again even if it were attempted because of the basic differences between Leo and the claimed invention, the result would not render the claimed invention obvious. Further the portion of Smith (col 10 lines 37-53) relied on by the Examiner is directed to "recertification performed in the field and again involves an outside certifying authority".

For all of the reasons set forth above, the rejection of claim 1 based on Leo in view of Smith should be withdrawn. The same is true of the rejections of claims 3, 7 and 11, 13 14 and 31, 18 and 22, 23, 29, 30, 32, 33, 34 and 36. All of these claims are dependent claims with the exception of claim 29. The dependent claims only add preferred features and cannot, in their failure to teach the elements of the independent claim, serve to render the claimed invention obvious. As to claim 29, as drafted, it defines a hybrid authentication system comprising distributed authentication structure which as cited above is not taught nor suggested by either Leo or Smith.

The rejection of the dependent claims, independent claim 29 and the claims dependent thereon should be withdrawn.

The Examiner had rejected claims 8 and 38 as unpatentable over Leo in view of Smith in further view of Dinker (35 USC §103(a)). Applicant respectfully requests reconsideration of this rejection. The Examiner admits that Leo in view of Smith does not disclose wherein said distributed authentication infrastructure requires a quorum of said plurality of nodes for enrolling a new entity into the hybrid authentication system and relies on Dinker as disclosing the quorum of said plurality of nodes enrolling a new entity (Dinker: see figure 3 and paragraph 0010), concluding that it would have been obvious to one of ordinary skill in the art to apply the teaching of the quorum method of Dinker into the system of Leo in view of Smith to enhance security because the pre-selected nodes have to vote and agree with each other in order for the new entity to get enrolled into the system.

As set forth above, Leo and Smith combined do not teach all of the required limitations of the independent claims and specifically claim 1; claims 8 and 38 are dependent claims directed to very specific features alleged to be found in Dinker. However, Dinker does not teach or suggest the required limitations of claim 1. Therefore the combination of Leo and Dinker fails to render obvious the applicant's invention as set forth in dependent claims 8 and 38. It should be noted that Dinker is directed to an entirely different system and as described operates so that in cluster 100 (group of nodes) which is configured to interact with one or more external clients (110 Fig 1A and 140 Fig. 1B) coupled to the cluster 100 via network 130 and during the interaction of the cluster 100 with clients, the clients may send the cluster requests for access to services provided by and/or data stored in the cluster, or request write access to update data already stored

in the cluster or to create new data within the cluster. Each node includes a consensus module and a serviceability module. In response to receiving a request to perform a serviceability update, a consensus module will send a vote to each other consensus module and depending on whether a quorum is indicated by the votes received from the consensus modules in the other nodes the serviceability module will perform the serviceability update. The skilled in the art would not consider making the modification to the combination of Leo and Smith as suggested by the Examiner because of the differences in subject matter and if he did, he would still, because of the differences in Leo from the claimed invention, not achieve the applicant's invention as claimed.

The Examiner has rejected claims 12 as unpatentable over Leo in view of Smith and further in view of Prabandham. Applicant respectfully requests reconsideration of this rejection. It is noted that claim 12 is a dependent claim drawn to a preferred feature. The Examiner has conceded that "Leo does not disclose in detail wherein said control server is coupled to a new entity and is utilized for verifying the identification of the new entity and enrolling said new entity into the hybrid authentication system, said central server producing a log for recording a plurality of failed authentication and a plurality of failed enrolments by said plurality of nodes" and relies on Prabandham to cure the omission. As Prabandham does not teach the elements of claim 1, it can not cure the deficiencies of Leo and Smith, and therefore the rejection of claim 12 should be withdrawn.

The Examiner has rejected claims 5-6, 15-17, 19-21, 24, 26-28, 35and 37 as unpatentable (35 USC 103a) over Leo in view of Smith in further view of Benantar. Applicant respectfully requests reconsideration of this rejection. At pages 8-12 of the office action, the Examiner admits in detail as to the claims involved what the combination of Leo and Smith does not disclose and relies on Benantar for curing these omissions.

All of the aforesaid claims are dependent claims and are directed to preferred features. As the elements of the independent claims are not suggested or taught by the Leo and Smith references, alone or in combination, the rejection should be withdrawn.

The Examiner has further rejected claims 9-10 under 35 USC 103 (a) over Leo in view of Smith in view of Dinker and further in view of Benantar. Applicant respectfully requests reconsideration of this rejection. In connection with the rejection of the dependent claims 9 and 10, the Examiner admits that Leo in view of Smith in view of Dinker does not explicitly disclose wherein each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature" and relies on Benantar and Dinker to cure this omission. As noted above, Leo, Smith and Dinker fail to disclose all the limitations of the independent claim 1 and as Benantar does not cure these deficiencies, this ground of rejection should be withdrawn. Again it is pointed out that it is the applicant's position that Benantar fails to teach what the Examiner relied on it to teach, i.e., "each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature." The paragraphs cited by the Examiner in Benantar

(0008, 0011 and 0037) are related to signing a certificate and no reference was made to each node of said quorum utilizing a partial key for partially signing a certificate to provide a full signature.

Claim 10 depends on claim 9.

The Examiner should withdraw this ground of rejection.

In view of the above, reconsideration and allowance of the claims in this case are requested.

SUMMARY

It is submitted that the application is in condition for allowance and notification thereof is respectfully requested. Should any issue remain to be resolved, Applicant requests that the Examiner telephone the undersigned attorney of record.

Respectfully Submitted,
Attorney for Applicant

Dated: January 23, 2009

/evelyn m. sommer/

Evelyn M. Sommer
Registration No. 19,603
OSTRAGER CHONG FLAHERTY
AND BROITMAN, PC
570 Lexington Avenue, 17th Floor
New York, NY 10022-6894
Phone: (212) 681-0600
Customer Number: 64722